AMENDMENTS TO THE CLAIMS

Please amend the claims of the present application as set forth below. In accordance with the PTO's revised amendment format, a detailed listing of all claims has been provided. A status identifier is provided for each claim in a parenthetical expression following each claim number. Changes to the claims are shown by strikethrough (for deleted matter) or underlining (for added matter).

Claims 1-35 were pending.

Claims 11-16, 24-26, 29, 33, and 35 are canceled.

No claims are added.

Claims 7-10, 17, 27, 30, and 32 are amended without prejudice.

Accordingly, claims 1-10, 17-23, 27, 28, 30-32, and 34 are pending.

1. (Original) A method, comprising:

associating a digital signature with a web page; and

delivering the web page to an electronic device capable of authenticating the digital signature and executing at least a portion of the web page after the digital signature is authenticated.

2. (Original) The method as recited in claim 1, wherein the associating further comprises attaching the digital signature to the web page.

3. (Original) The method as recited in claim 1, further comprising:

determining if the web page includes code to invoke a control object; and

deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object.

4. (Original) The method as recited in claim 1, wherein the web page includes a confirmation module that is used by the electronic device to authenticate the digital signature.

5. (Original) The method as recited in claim 1, wherein the web page contains script that, when executed, invokes executable code that is executed on the electronic device executing the web page.

6. (Original) The method as recited in claim 1, wherein the web page is generated in an active server page (ASP) environment.

7. (Currently amended) A method, comprising:

receiving a web page from a server, the web page containing executable script that, when executed, invokes a control object, the web page having a ~~segment~~ digital signature that can be used to identify ~~uniquely identifies~~ a source of the web page;

determining whether ~~authenticating~~ the source of the web page is authentic via the digital signature; and

in an event that the source of the web page is authentic, displaying the web page and invoking the control object~~if the web page is authenticated~~.

8. (Currently amended) The method as recited in claim 7, further comprising:

in an event that the source of the web page is not authentic, refusing to invoke the control object.~~determining if the source of the web page is authorized to invoke the control object; and~~

~~displaying the web page only if the source of the web page is authorized to invoke the control object.~~

9. (Currently amended) The method as recited in claim 7, wherein the ~~authenticating~~ determining further comprises ~~authenticating the source of the web page to~~ identifying the source of the web page.

10. (Currently amended) The method as recited in claim 7, further comprising:

designating one or more authorized sources from which a web page that invokes a control object may be received; and

executing script contained in the web page only if the determining ~~authenticating the source of the web page~~ indicates that the web page was received from one of the one or more ~~an~~ authorized sources.

11. – 16. (Cancelled)

17. (Currently amended) A system, comprising:

a web browser configured to access a web page having a digital signature;

a processor configured to execute script contained in the web page;

an executable control object that may be invoked by the script in the web page and is executable on the processor; and

a confirmation module configured to authenticate the digital signature to determine based on authenticity of the digital signature, whether the control object should be invoked~~; and~~

~~wherein the confirmation module is called when the control object is invoked by the script, the control object executing only if the confirmation module authenticates the digital signature~~.

18. (Original) The system as recited in claim 17, wherein the confirmation module is called by the control object.

19. (Original) The system as recited in claim 17, wherein the confirmation module is included in the control object.

20. (Original) The system as recited in claim 17, wherein the confirmation module is included in the web browser.

21. (Original) The system as recited in claim 17, wherein the confirmation module is further configured to determine if the web page comes from a source that is authorized to invoke the control object and the control object is invoked only if the source of the web page is authorized to invoke the control object.

22. (Original) The system as recited in claim 17, wherein the confirmation module is called by the web page prior to the web page invoking the control object.

23. (Original) The system as recited in claim 17, wherein the digital signature module is not invoked if the web page does not have a digital signature.

24. – 26. (Cancelled)

27. (Currently amended) A web browser contained on a computer-readable medium of a client computer, comprising computer-executable instructions that, when executed by the client computer, perform the following:

determining if a web page contains instructions to invoke a control object;

determining if the web page has an associated digital signature;

in an event that the web page has an associated digital signature, authenticating the web page using ~~a~~ the digital signature; and

invoking the control object if the source of the web page is authenticated.

28. (Original) The web browser as recited in claim 27, further comprising:

determining if the web page contains executable script to invoke a control object; and

wherein the authenticating the web page further comprises authenticating the web page only if the web page contains executable script to invoke a control object.

29. (Cancelled)

30. (Currently amended) The web browser as recited in claim 27, ~~wherein the control object is not invoked if the web page does not include a digital signature~~further comprising in an event that the web page does not have an associated digital signature, refusing to invoke the control object.

31. (Original) The web browser as recited in claim 27, further comprising instructions to determine if an authenticated web page comes from a source that is authorized to invoke the control object.

32. (Currently amended) A control object stored in a computer-readable medium, comprising computer-executable instructions that, when executed on a computer, perform the following:

authenticating a web page that invokes the control object, wherein the authenticating is performed based on a digital signature associated with the web page; and

executing a data-handling task on the computer if the web page is` determined to be authentic.

33. (Cancelled)

34. (Original) The control object as recited in claim 32, further comprising instructions to determine if a source of the web page is authorized to invoke the data-handling task prior to executing the data-handling task.

35. (Cancelled)